GUIDELINE FOR DATA HANDLING

PURPOSE

The purpose of this document is to provide a guide for protecting internal and customer data from unauthorized access or disclosure. Every member of Moment Team AS is expected to follow appropriate security precautions to protect sensitive data and avoid compromising the privacy rights of customers.

SCOPE

This guideline applies to Moment employees, affiliates, associates, contractors, consultants, and anyone accessing Moment owned data or managed data, in physical or electronic format.

Only authorized persons have access to internal and customer data. Access rights are carefully determined and given to employees that require access in order to perform daily work duties.

CONTACT

Any questions regarding this guideline can be directed to the company's information security liaison. If you have any specific questions, please contact privacy@moment.team.

UNDERSTANDING DATA TYPES

It is important to understand the difference between public, internal, and personal data.

Public data is data that is purposefully made available to the public. This includes but is not limited to:

Advertising, product and service information, directory listings, job postings, and press releases.

Internal data is any protected data pertaining to the business, its employees and customers, either owned or managed by Moment. While some forms of internal data can be made available to the public under some circumstances, the data is not freely disclosed. This includes but is not limited to:

Employee phone numbers, HR information, financial and investment information, marketing and sales information.

Personal data is any data relating to an identified or identifiable individual.
This includes but is not limited to:

Name, phone number, email address, location, occupation, social identity, photos, and other identifying information.

We must ensure that personal and internal data is protected from data breaches. A big part of this is understanding what qualifies as personal data, and the appropriate ways of receiving this data going forward. If you are uncertain what category something falls under, or how to handle it, contact the information security liaison or your immediate supervisor.

Personal data may only be used for its intended purpose, in the way that the data controller has consented it to be used. Do not request personal information via email, instant message, chat or unsecured file transfer (such as FTP).

Employees should be mindful if working in a public place (e.g. a cafe or airport) that no confidential data or personal data is showing while doing so. Speaking about confidential information or personal data outside of work, and outside of its intended purpose is strictly forbidden. Do not discuss or display confidential/personal data in an environment where it may be viewed or overheard by unauthorized individuals.

Any breach or mishandling of data must be immediately reported to either the information security liaison or your immediate supervisor, as this must be reported further to the data controller. Failure to do so may result in disciplinary action.

Any personal, internal, or customer data received into Moment or its sub-processors is to remain confidential, in following with GDPR regulations and local laws.